(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3426006 A1**

(51) Int. Cl. 3: G 07 C 9/00

(21) Aktenzeichen: P 34 26 006.4
(22) Anmeldetag: 14. 7. 84
(43) Offenlegungstag: 7. 2. 85

DE 3426006 A1

(30) Unionspriorität: (32) (33) (31)
29.07.83 FR 8312528

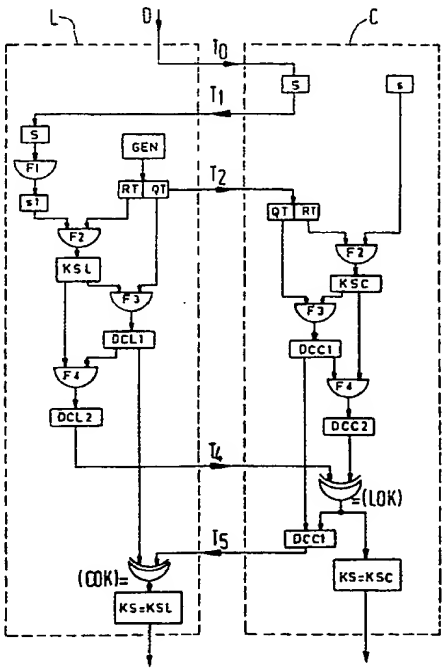
(71) Anmelder:
N.V. Philips' Gloeilampenfabrieken, Eindhoven, NL

(74) Vertreter:
Poddig, D., Dipl.-Ing., Pat.-Ass., 2000 Hamburg

(72) Erfinder:
Robert, Serge, Jouy en Josas, FR; Cahart, Olivier, Versailles, FR; le Marchant, Pierre, Clamart, FR

(54) Authentisierungsanordnung zwischen einem Scheckkartenleser und einer Scheckkarte beim Datenaustausch

Authentisierungsanordnung zwischen einem Scheckkartenleser und einer Scheckkarte beim Datenaustausch.
Eine Reziprokauthentisierungsanordnung zwischen zwei Gruppen elektronischer Einheiten, die für den Austausch von Daten miteinander verbindbar sind.
Die Anordnung erzeugt periodisch einen variablen Zugriffsschlüssel für die Verschlüsselung vertraulicher Austauschvorgänge.




BUNDESDRUCKEREI 12. 84 408 066/521 7/60

PATENTANSPRÜCHE:

1. Reziprokauthentisierungs- und Datenaustauschanordnung mit einem ersten Lesersatz und einem zweiten Scheckkartensatz, die mit jedem Leser frei verbindbar ist, wobei jede Scheckkarte und jeder Leser Verarbeitungs- und Speichermittel enthalten, die in angeschlossenem Zustand zum Speichern, Verarbeiten und Erzeugen von Daten in der Scheckkarte und von Daten im Leser, zum Abwandeln der Daten, zum Übertragen der Daten auf den Leser und auf die Scheckkarte und weiter zum Überprüfen der nach der Übertragung empfangenen Daten dienen, wobei die Anordnung ebenfalls Detektormittel zum Prüfen der Übereinstimmung der nach der Überprüfung erzeugten Signale und vorkommendenfalls zur Ermöglichung weiterer Datenaustauschvorgänge zwischen der miteinander verbundenen Scheckkarte und dem Leser, deren Verbindung auf diese Weise authentisiert wird, enthält, dadurch gekennzeichnet, dass die in jeder Karte gespeicherten Daten insbesondere einen ersten Geheimcode (S), der für jede Karte spezifisch ist, und einen zweiten Geheimcode (s) enthält, der durch einen Bi-Univok-(F1)- und eine Umkehrungs-($F1^{-1}$)-Umsetzungsfunktion mit dem ersten Code (S) verknüpft und nicht für jede Karte spezifisch ist, wobei der Prozessor eine für jede Karte nicht-spezifische zweite (F2), dritte (F3) und vierte (F4) Umsetzungsfunktion und in jedem Leser eine weitere erste Umsetzungsfunktion, die gleich der ersten Umsetzungsfunktion (F1) ist, die die zwei Geheimcodes (S und s) jeder Karte miteinander verknüpft, einen Zufallsgenerator (GEN) zum Erzeugen einer ersten (RT) und einer zweiten (QT) Zufallszahl bei jedem Anschluss einer Karte, eine weitere zweite, eine weitere dritte und eine weitere vierte Umsetzungsfunktion enthält, die gleich den zweiten (F2), dritten (F3) bzw. vierten (F4) Umsetzungsfunktionen sind, wobei der erste Geheimcode (S) nach dem Empfang eines Startsignals (T0) aus dem Leser in der Karte von der Karte auf den Leser übertragen wird (T1), wobei die Umsetzungsfunktion (F1) des Lesers dazu den ersten Geheimcode (S) in einen Geheimcode (s1) umsetzt, wonach in der Folge der Umsetzung (T2) der ersten und zweiten Zufallszahlen aus dem Leser in die Karte die Prozessoren der Karte und des Lesers stellenweise parallel und jeweilig die zweite Umsetzungsfunktion

(F2) einsetzen: einerseits bei RT und s zum Erhalten eines Kartenzugriffsschlüssels KSC und andererseits bei RT und s1 zum Erhalten eines Leserzugriffsschlüssels KSL, wonach die dritte Umsetzungsfunktion (F3) einerseits bei QT und KSC zum Erhalten erster Vergleichsdaten DCC 1 in der Karte und andererseits bei QT und KSL zum Erhalten erster Verleichsdaten DCL 1 im Leser eingesetzt wird, wonach die vierte Umsetzungsfunktion (F4) einerseits bei DDC 1 und KSC zum Erhalten zweiter Vergleichsdaten DCC 2 in der Karte und andererseits bei DCL 1 und KSL zum Erhalten zweiter Vergleichsdaten DCL 2 im Leser eingesetzt wird, wobei nach der Übertragung (T4) von DCL 2 aus dem Leser in die Karte der Überprüfer der Karte feststellt, dass DCL 2 und DCC 2 gleich sind (LOK), und in einem solchen Fall die Übertragung (T5) von DCC 1 von der Karte in den Leser genehmigt, wobei der Überprüfer des Lesers feststellt, dass DCC 1 und DCL 1 gleich sind (COK), und in einem solchen Fall weitere Datenaustauschvorgänge zwischen der Karte und dem Leser genehmigt, wobei ein Zugriffsschlüssel KS, der so authentisiert ist, dass er gleich dem (KSL) des Lesers und dem (KSC) der Karte ist, derart gespeichert wird, dass er zur Gewährleistung der Vertraulichkeit der Datenaustauschvorgänge durch Verschlüsselung zur Verfügung steht.

2. Reziprokauthentisierungsanordnung nach Anspruch 1, dadurch gekennzeichnet, dass die vier Umsetzungsfunktionen (F1, F2, F3, F4) untereinander, oder auch je zwei und zwei, oder je drei und drei gleich sein können.

3. Reziprokauthentisierungsanordnung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Zufallszahlengenerator (GEN) in der Karte angeordnet ist, wobei die Übertragung (T2) der ersten (RT) und der zweiten (QT) Zufallszahlen von der Karte auf den Leser erfolgt, so dass die Übertragungen T1 und T2 durch nur eine einzige Übertragung T12 darstellbar ist.

4. Reziprokauthentisierungsanordnung nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, dass das Startsignal T0 aus der Karte herrührt, so dass es nur eine einzige Übertragung (T01) mit T1 oder eine einzige Übertragung (T012) mit T1 und T2 bewirkt.

5. Reziprokauthentisierungsanordnung nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass der Prozessor des Lesers schneller als der Prozessor der Karte ist, wobei der Leser in einen Wartezustand (W) eintritt, und der Prozessor der Karte Mittel zur Benachrichti-

gung (T3) des Lesers enthält, dass die Umsetzungsfunktionen in der Karte durchgeführt sind, wobei die Übertrager dieses Lesers und dieser Karte nach dem Empfang dieser Nachricht über die Durchführung der Funktionen die Wirkung für die Übertragung (T4) dieser Vergleichsinformation aus dem Leser zur Karte und umgekehrt (T5) einleitet.

6. Reziprokauthentisierungsanordnung nach Anspruch 1, 2, 3, 4 oder 5, dadurch gekennzeichnet, dass die nicht für jede Karte spezifische Funktion (F1) für ein Paar miteinander verbindbarer Leser-Untersätze spezifisch ist, so dass andere Datenaustauschvorgänge zwischen einem Element eines der Untersätze dieses Paars und einem Element eines anderen Paars mit einer spezifisch verschiedenen Funktion (F1', F1", ...) nicht genehmigt wird.

7. Reziprokauthentisierungsanordnung nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass das Startsignal T0 während der Datenaustauschvorgänge zwischen einer Karte und einem Leser, die miteinander verbunden bleiben, erneuert wird, welche Erneuerung so oft wiederholt wird, als zur Gewährleistung der Vertraulichkeit der Vorgänge notwendig erachtet wird, wobei jede Erneuerung die Erzeugung eines neuen Zugriffsschlüssels KS für die Verschlüsselung der Austauschvorgänge bedeutet.

8. Reziprokauthentisierungsanordnung nach einem der vorangehenden Ansprüche zur Verwendung für einen Dialog zwischen Datenverarbeitungssystemen mit Prozessoren und Speichern.

3426006

Authentisierungsanordnung zwischen einem Scheckkartenleser und einer Scheckkarte beim Datenaustausch.

Die Erfindung betrifft eine Reziprokauthentisierungs- und Datenaustauschanordnung mit einem ersten Lesersatz und einem zweiten Scheckkartensatz, die mit jedem Leser frei verbindbar ist, wobei jede Scheckkarte und jeder Leser Verarbeitungs- und Speichermittel enthalten, die in angeschlossenem Zustand zum Speichern, Verarbeiten und Erzeugen von Daten in der Scheckkarte und von Daten im Leser, zum Abwandeln der Daten, zum Übertragen der Daten auf den Leser und auf die Scheckkarte und weiter zum Überprüfen der nach der Übertragung empfangenen Daten dienen, wobei die Anordnung ebenfalls Detektormittel zum Prüfen der Übereinstimmung der nach der Überprüfung erzeugten Signale und vorkommendenfalls zur Ermöglichung weiterer Datenaustauschvorgänge zwischen der miteinander verbundenen Scheckkarte und dem Leser, deren Verbindung auf diese Weise authentisiert ist, enthält.

Eine derartige Anordnung ist aus der US-PS 3 806 874 bekannt und dient zum Authentisieren einer Verbindung beispielsweise zwischen einer Bankscheckkarte und einem Scheckkartenleser vor dem Datenaustausch oder vor der Durchführung von Dienstleistungen, die nur nach einer gegenseitigen Überprüfung zugänglich sind: Ist die Scheckkarte eine "Original"-Karte für den Leser?; Ist der Leser ein "origineller" Leser für die Karte? Diese Überprüfung dient zum Ausschliessen der Möglichkeit, eine Originalkarte mit Hilfe eines nicht originellen Lesers oder einen originellen Leser mit Hilfe einer nicht originellen Karte "sprechen" zu lassen wodurch es einem Betrüger möglich wäre, Scheckkarten geeigneter Güte zu fälschen.

In dieser Anordnung wird ein elektronischer Prozessor verwendet, wie er in der Datenverarbeitungsindustrie benutzt wird; seine Verwendung beschränkt sich nicht zu bankbezogenen Transaktionen: Jeder Datenaustausch zwischen Datenverarbeitungsanordnungen lässt sich mittels einer derartigen Authentisierungsanordnung überprüfen.

Eine der Ausführungformen der Authentisierungsanordnung gemäss der Beschreibung in der erwähnten Patentschrift enthält einen Zufallszahlengenerator (51), der im Leser angeordnet ist. Der Aufbau ist auf diese Weise für einen künftigen Betrüger kompliziert, der sich die

Authentisierungsaustauschvorgänge auf den Leiter 37 und 45 des bekannten Systems ansieht, aber die nachfolgenden Datenaustauschvorgänge sind nach wie vor ungeschützt, so dass nach der Authentisierung einer Originalkarte der Betrüger sie gegen eine andere Karte austauschen und so in das System einbrechen könnte. Ausserdem impliziert eine Schutzmassnahme nach der Beschreibung in der erwähnten Patentschrift (Figur 12) eine verhältnismässig geringe Abmessung der geheimen Kartenschaltungen. Dies bedeutet eine Einschränkung, die sich nicht mit der Erweiterung der Bedeutung des Begriffs "Karte" für Datenverarbeitungssysteme nach obiger allgemeinen Beschreibung verträgt.

Der Erfindung liegt die Aufgabe zugrunde, diese Nachteile zu beseitigen.

Diese Aufgabe wird mit einer Authentisierungs- und Datenaustauschanordnung erfindungsgemäss dadurch gelöst, dass die in jeder Karte gespeicherten Daten insbesondere einen ersten Geheimcode (S), der für jede Karte spezifisch ist, und einen zweiten Geheimcode (s) enthält, der durch einen Bi-Univok-(F1)- und eine Umkehrungs-($F1^{-1}$)-Umsetzungsfunktion mit dem ersten Code (S) verknüpft und nicht für jede Karte spezifisch ist, wobei der Prozessor eine für jede Karte nichtspezifische zweite (F2), dritte (F3) und vierte (F4) Umsetzungsfunktion und in jedem Leser eine weitere erste Umsetzungsfunktion, die gleich der ersten Umsetzungsfunktion (F1) ist, die die zwei Geheimcodes (S und s) jeder Karte miteinander verknüpft, einen Zufallsgenerator (GEN) zum Erzeugen einer ersten (RT) und einer zweiten (QT) Zufallszahl bei jedem Anschluss einer Karte, eine weitere zweite, eine weitere dritte und eine weitere vierte Umsetzungsfunktion enthält, die gleich den zweiten (F2), dritten (F3) bzw. vierten (F4) Umsetzungsfunktionen sind, wobei der erste Geheimcode (S) nach dem Empfang eines Startsignals (T0) aus dem Leser in der Karte von der Karte auf den Leser übertragen wird (T1), wobei die Umsetzungsfunktion (F1) des Lesers dazu den ersten Geheimcode (S) in einen Geheimcode (s1) umsetzt, wonach in der Folge der Umsetzung (T2) der ersten und zweiten Zufallszahlen aus dem Leser in die Karte die Prozessoren der Karte und des Lesers stellenweise parallel und jeweilig die zweite Umsetzungsfunktion (F2) einsetzen: einerseits bei RT und s zum Erhalten eines Kartenzugriffsschlüssels KSC und andererseits bei RT und s1 zum Erhalten eines Leserzugriffsschlüssels KSL, wonach die dritte Umsetzungsfunktion (F3) einerseits bei QT und KSC zum Erhalten erster Vergleichsdaten DDC 1 in der Karte und andererseits bei QT un KSL

zum Erhalten erster Vergleichsdaten DCL 1 im Leser eingesetzt wird, wonach die vierte Umsetzungsfunktion (F4) einerseits bei DCC 1 und KSC zum Erhalten zweiter Vergleichsdaten DDC 2 in der Karte und andererseits bei DCL 1 und KSL zum Erhalten zweiter Vergleichsdaten DCL 2 im Leser eingesetzt wird, wobei nach der Übertragung (T4) von DCL 2 aus dem Leser in die Karte der Überprüfer der Karte feststellt, dass DCL 2 und DCC 2 gleich sind (LOK), und in einem solchen Fall die Übertragung (T5) von DDC 1 von der Karte in den Leser genehmigt, wobei der Überprüfer des Lesers feststellt, dass DDC 1 und DCL 1 gleich sind (COK), und in einem solchen Fall weitere Datenaustauschvorgänge zwischen der Karte und dem Leser genehmigt, wobei ein Zugriffsschlüssel KS, der so authentisiert ist, dass er gleich dem (KSL) des Lesers und dem (KSC) der Karte ist, derart gespeichert wird, dass er zu Gewährleistung der Vertraulichkeit der Datenaustauschvorgänge durch Verschlüsselung zur Verfügung steht.

Der Zufallszahlengenerator wird also durchaus für die Erzeugung eines Zugriffsschlüssels benutzt, der nie auf der Übertragungsleitung oder den Leitungen von einem Betrüger feststellbar ist. Ausserdem kann der Betrüger, weil der Zugriffsschlüssel von einer Authentisierung zum anderen ungleich ist und die Funktionen F1, F2, F3 und F4 besonders kompliziert sein können, nie einige Kenntnis daraus in bezug auf den ersten Geheimcode S bekommen, die er herausbekommen könnte, indem er eine Originalkarte "sprechen" liesse. Ebensowenig kann er Kenntnis daraus in bezug auf die Zufallszahlen RT und QT und/oder die zweiten Vergleichsdaten DCL 2 des Lesers ableiten, die er herausbekommen könnte, indem er einen Originalleser "sprechen" liesse. Also wird es für ihn nicht möglich sein, den Zugriffsschlüssel zu erhalten, den er zum Verfolgen des Datenaustauschdialogs benötigte.

Nachstehend ist eine vorteilhafte Abwandlung beschrieben.

Zum Erhalten eines wirtschaftlichen, wenn auch weniger wirksamen Systems ist ein Reziprokauthentisierungssystem nach der Erfindung insbesondere dadurch gekennzeichnet, dass die vier Umsetzungsfunktionen (F1, F2, F3, F4) gegenseitig gleich, je zwei und zwei oder drei und drei gleich sein können.

Der Prozessor des Lesers wie auch der der Karte sind dadurch einfacher und also preisgünstiger, jedoch sind dabei die Funktion(en) leichter ausfindig zu machen. Die Wahl der Funktion(en) ist auf Basis des verlangten Schutzmasses zu treffen.

Eine andere Ausführungsform des erfindungsgemässen Reziprokauthentisierungssystem ist dadurch gekennzeichnet, dass der Zufallszahlengenerator (GEN) in der Karte angeordnet ist, wobei die Übertragung (T2) der ersten (RT) und der zweiten (QT) Zufallszahl von der Karte zum Leser erfolgt, so dass die Übertragungen T1 und T2 durch eine einzige Übertragung T12 darstellbar sind.

Der Prozessor der Karte kann dabei etwas umfangreicher und also teurer und weniger kompakt sein. Jedoch wird eine höhere Geschwindigkeit erreicht, weil die zwei Übertragungen auf diese Weise zu einer einzigen Übertragung kombiniert werden.

Die vorliegende Erfindung bietet weitere Vorteile, und andere Abwandlungen sind ebenfalls möglich. Ausführungsbeispiele der Erfindung werden nachstehend anhand der Zeichnung näher erläutert. Es zeigen

Figur 1 die Grundausführung der Authentisierungsanordnung,

Figur 2 eine Gruppe abgeleiteter Ausführungsformen dieser Anordnung.

Die verschiedenen Elemente sind in beiden Figuren 1 und 2 mit übereinstimmenden Bezugsziffern bezeichnet. Die Umsetzungsfunktionen sind mit Halbkreisen angegeben. Die gespeicherten Daten, die aus den Funktionen übertragen oder daraus abgeleitet werden, sind mit Rechtecken angegeben. Ununterbrochene Linien stellen den logischen Datenfluss dar im Gegensatz zur physikalischen Anordnung der elektrischen Leiter, die für ein gutes Verständnis der Erfindung nicht eingehend beschrieben zu werden brauchen.

In Figur 1 ist ein Leser L in einer gestrichelten Linie und eine Karte C in einer gestrichelten Linie in dem Zustand dargestellt, in dem sie mittels (nicht dargestellter) Verbindungen miteinander verbunden sind, zum Beispiel mittels Verbindungen gemäss der Norm AFNOR CF/TC97/SC17/GT4, veröffentlicht durch die Association Française pour la Normalisation, Tour EUROPA, CEDEX 792080, Paris la Défence, France.

Sobald die Verbindung zwischen Karte und Leser hergestellt ist, erzeugt ein Kartendetektor, z.B. ein Streckenendedetektor, ein Signal D, das auf die Karte übertragen wird (T0); jede Karte ist so ausgelegt, dass sie einen Dauerspeicher enthält, in dem ein erster Geheimcode S und ein zweiter Geheimcode s gespeichert sind, welche beiden Codes für jede Karte spezifisch sind, die sich dadurch auszeichnet.

S und s werden durch die Umsetzungsfunktion $F1^{-1}$ miteinander verknüpft: $S = F1^{-1}(s)$. Das bedeutet, dass S auf der Basis von s berechnet wird, wenn die Karte hergestellt wird. Die Funktion $F1^{-1}$ ist eine Funktion, deren Umkehrfunktion F1 bekannt und für alle Karten und alle Leser gleich ist.

Das Signal D ist das Startsignal für die Reziprokauthentisierungsanordnung. Beim Empfang dieses Signals D überträgt die Karte den Code S auf den Prozessor des Lesers, der darauf die Funktion F1 zum Erhalten eines Ergebnisses s1, anwendet das gleich dem Geheimcode s sein soll, wenn eine Originalkarte und ein Originalleser miteinander verbunden sind. Die Bezeichnung s1 dient zur Betonung der Unterschiede, die bei einem Betrug oder einem möglichen Fehler auftreten können.

Wenn davon ausgegangen wird, dass der Zufallszahlengenerator GEN von Prozessor des Lesers unabhängig ist, was nicht unbedingt notwendig ist, erzeugt der Generator zwei Zufallszahlen RT und QT, die als solche im Leser gespeichert sind und auf die Karte übertragen werden, in der sie ebenfalls als solche gespeichert sind.

Die Speicher der Karte und des Lesers enthalten somit drei identische Daten: RT, QT und s = s1.

Die Prozessoren der Karte und des Lesers sind zum Enthalten der gleichen Umsetzungsfunktionen F2, F3 und F4 ausgelegt, die wie folgt auf die gleichen Daten angewandt werden (siehe Figur 1):

- F2 in der Karte wird auf RT und auf s angewandt, und erzeugt eine Information, die mit dem Kartenzugriffsschlüssel KSC bezeichnet wird,
- F2 im Leser wird auf RT und s1 angewandt, und erzeugt eine Information, die mit dem Leserzugriffsschlüssel KSL bezeichnet wird,
- F3 in der Karte wird auf QT und KSC angewandt, und erzeugt eine erste Vergleichsinformation DCC 1 in der Karte,
- F3 im Leser wird auf QT und KSL angewandt, und erzeugt eine erste Vergleichsinformation DCL 1 im Leser,
- F4 in der Karte wird auf DCC 1 und KSC angewandt, und erzeugt eine zweite Vergleichsinformation DCC 2 in der Karte,
- F4 im Leser wird auf DCL 1 und KSL angewandt, und erzeugt eine zweite Vergleichsinformation DCL 2 im Leser.

Die Speicher der Karte und des Lesers enthalten jetzt je drei Informationen: KSC, DCC 1, DCC 2 und KSL, DCL 1, DCL 2, die normalerweise paarweise gleich sein sollen. Da sie die komplizierteste

Information durch die Anwendung der grössten Anzahl von Funktionen ist, wird die zweite Vergleichsinformation aus dem Leser auf die Karte übertragen (T4). Wenn das Vergleichsergebnis von DCL 2 und DCC 2 ungenügend ist, "schweigt" die Karte und die Authentisierung erfolgt nicht. Übereinstimmung bedeutet jedoch, dass die Karte den Leser als Originalleser (= LOK) anerkennt, so dass der Kartenzugriffsschlüssel für die nachfolgende Austauschvorgänge (KS = KSC) als gültig bewertet und die erste Vergleichsinformation (DCC 1) auf den Leser übertragen wird (T5), der bei Übereinstimmung mit DCL 1, selbst wieder die Karte als Originalkarte (= COK) anerkennt und den Zugriffsschlüssel (KS = KSL) als gültig bewertet. Sodann ist die Anordnung für jeden nachfolgenden Datenaustausch zwischen der Karte und dem Leser bereit und der Leser also gegenseitig authentisiert. Es ist ein wesentlicher Vorteil, dass die Nachrichten dieser Datenaustauschvorgänge mit einem Schlüssel KS verschlüsselt werden, der nie Gegenstand einer Übertragung über eine Leitung sein wird und von der einen Authentisierung zur anderen verschieden sein wird.

Die Tatsache, dass weder s noch KS je übertragen wird, erlaubt die Verwendung verhältnismässig ungeschützter Verbindungen. Daher sind dabei die physikalischen Abmessungen der Prozessoren und Speicher der Karte nicht eingeschränkt.

Jedoch kann es wünschenswert sein, die Anzahl der Funktionen, zum Beispiel aus Kostenerwägungen, zu beschränken. Dies kann nur auf Kosten der Sicherheit gehen, aber in bestimmten Fällen ist es vorteilhaft, den Prozessor nur für eine Funktion F zu implementieren, die immer angewandt wird: F = F1 = F2 = F3 = F4. Auch ist es möglich, nur zwei Funktionen wie in Figur 2 aufrechtzuerhalten, in der F3 den gleichen Prozessor wie F2 verwendet, also F3 = F2, und in der F4 den gleichen Prozessor wie F1 verwendet, also F4 = F1. Es sind aucn weitere Kombinationen möglich.

Auf andere Weise lässt sich die Anordnung durch die Verwirklichung des Zufallszahlengenerators (GEN) in der Karte, wie in Figur 2 angegeben, komplizierter machen, wobei jedoch die Anzahl der Umsetzungsfunktionen nicht gleichzeitig verringert zu werden braucht. Wenn der Generator in der Karte angeordnet ist, müssen die Zufallszahlen QT und RT auf den Leser übertragen werden und die Übertragung erfolgt in einer Richtung, die der Richtung in Figur 1 entgegengesetzt ist. Jedoch kann diese Übertragung gleichzeitig mit der Übertragung (T1)

von S erfolgen, wie sie in Figur 2 mit der Übertragung T12 dargestellt ist. Es wird also eine Übertragung erspart und die Authentisierung geht schneller.

Ebenso kann das Startsignal in einer nicht dargestellten Ausführungsform aus der Karte herrühren, in welchem Fall die Übertragungen T0, T1 und T2 nur eine einzige Übertragung T012 bilden. Dies würde insbesondere der Fall sein in einem Datenverarbeitungssystem, in dem die "Karte" grösser ist als das übliche Format einer Scheckkarte, wie z.B. in der Form eines in der Hand gehaltenen Computerterminals. Ein derartiger Terminal könnte bestimmt einen Detektor D enthalten.

Bei Zahlungskarten oder anderen Karten mit verhältnismässig geringen Abmessungen kann der Prozessorbetrieb der Karte viel langsamer als der des Lesers sein. In diesem Fall ist für einen Leser vorteilhafter, in eine Warteschleife einzutreten (W), bis die Karte ein Vollendungssignal (T3) zur Durchführung der Übertragung (T4) der erwähnten Vergleichsinformation DCL 2 des Lesers aussendet. Vorzugsweise "spricht" der Leser als erster (T4 vor T5), weil dadurch die Möglichkeit zum Betrug für einen künftigen Betrüger stark kompliziert wird. Selbstverständlich lässt sich die Übertragungsfolge ohne grosse Schwierigkeiten umkehren (T5 vor T4).

Wie bereits erwähnt, ist es vorteilhaft, dass nicht nur verhältnismässig kleine Karten, aber auch grössere Systeme angeschlossen und authentisiert werden können. Zum Ausnutzen des Vorteils dieser neuen Möglichkeit und weiter zum Vergrössern der Anzahl verschiedener Anwendungsmöglichkeiten von Karten mit einem Speicher ist die Funktion F1, die S mit s verknüpft, vorzugsweise spezifisch für zwei Unteranordnungen, die miteinander verbunden werden können. So kann zum Beispiel eine von der Bank A abgegebene Karte nicht von einem von der Bank B abgegebenen Leser authentisiert werden: $F1 \neq F1' \neq F1'' \ldots$ .

Wenn der Dialog, der der Authentisierung folgt und den Zugriffsschlüssel für die Verschlüsselung verwendet, besonders lang oder vertraulich ist, kann es vorteilhaft sein, den Schlüssel periodisch zu ändern, ohne eine Trennung erforderlich zu machen. Zu diesem Zweck leitet der Leser oder die Karte auf der Basis der abgelaufenen Zeit oder einer Anzahl übertragener Nachrichten oder auf andere Weise die Simulierung des Startsignals T0 ein, wodurch neue Authentisierungen eingeleitet werden, die jedesmal einen neuen Schlüssel für den Zugriff und für die Verschlüsselung erzeugen, so dass der Dialog zwischen den gleichen zwei,

die angeschlossen bleiben, fortgesetzt wird. Dadurch wird ein künftiger Betrüger eine nahezu unlösliche Aufgabe haben, weil der Schlüssel geändert wird, ohne dass es ihm bekannt wird.

Num.:
Int. Cl.:
Anmeldetag:
Offenlegungstag:

34 26 006
G 07 C 9/00
14. Juli 1984
7. Februar 1985



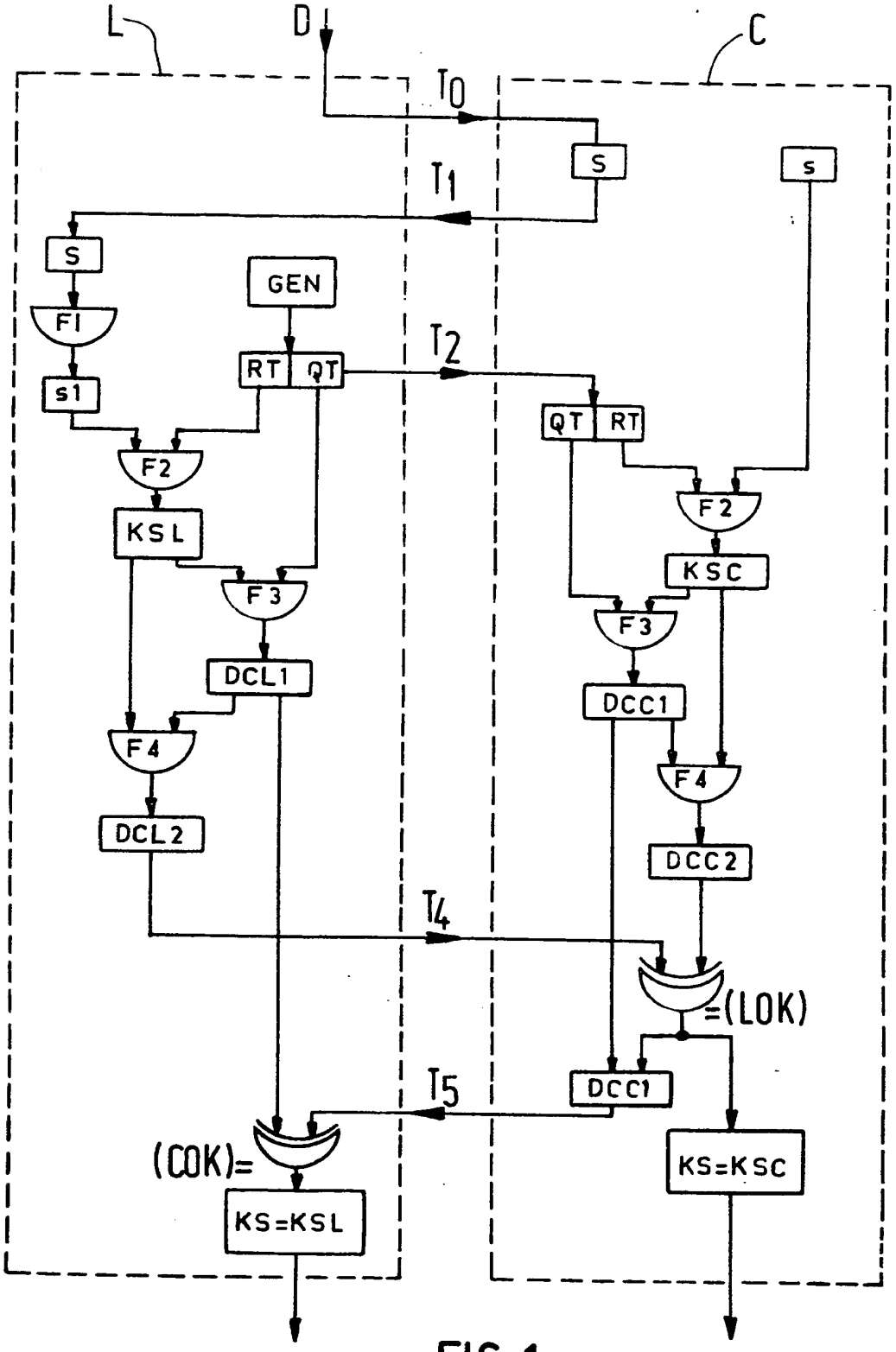



FIG.1

1-II-PHF 83-565

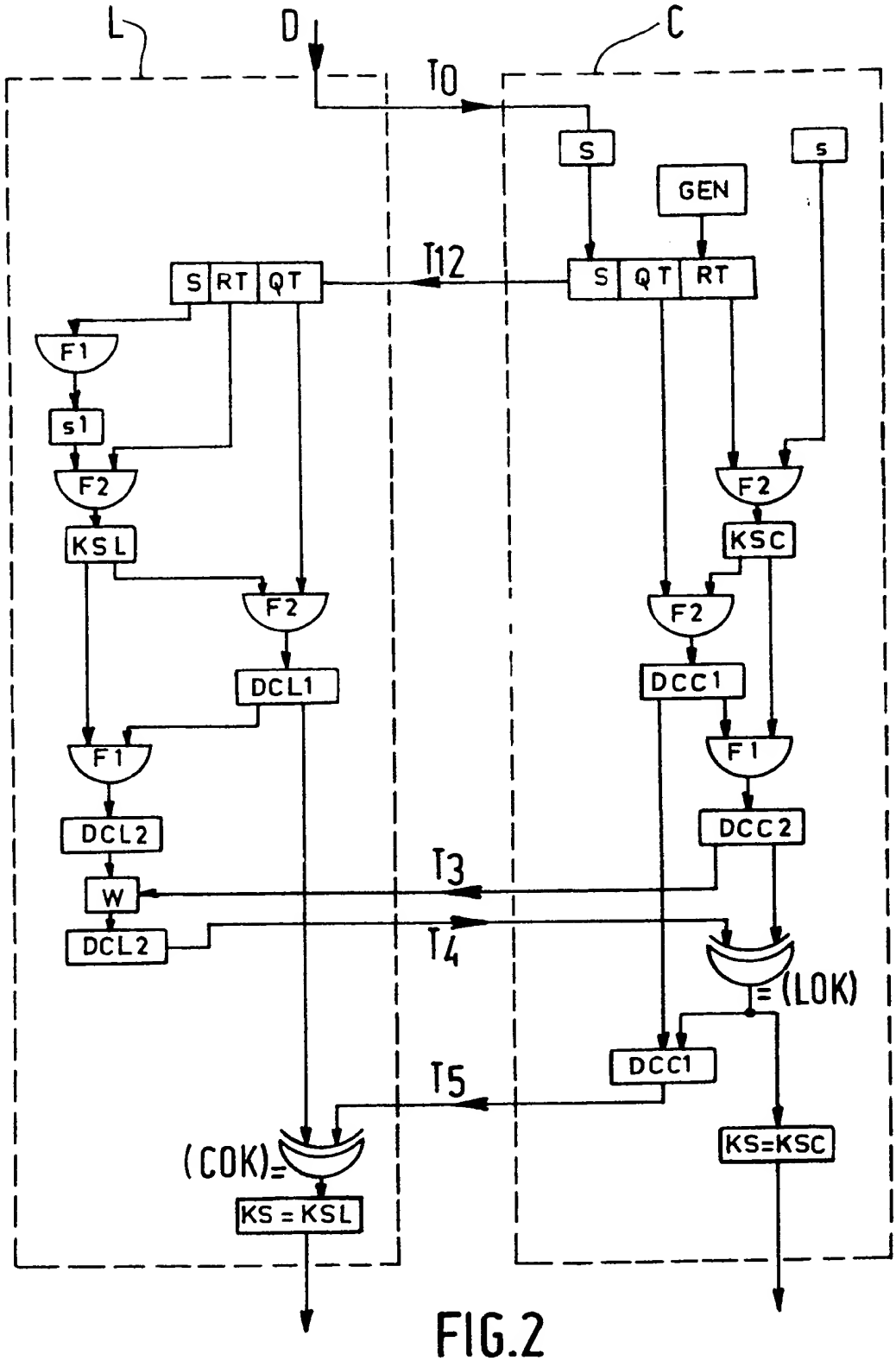



FIG.2